House of Commons

European Scrutiny Committee

Fortieth Report of Session 2019–21

Documents considered by the Committee on 17 March 2021

Report, together with formal minutes

Ordered by The House of Commons
to be printed 17 March 2021

HC 229-xxxv
Published on 23 March 2021
by authority of the House of Commons

Notes

Numbering of documents

Three separate numbering systems are used in this Report for European Union documents:

Numbers in brackets are the Committee's own reference numbers.

Numbers in the form "5467/05" are Council of Ministers reference numbers. This system is also used by UK Government Departments, by the House of Commons Vote Office and for proceedings in the House.

Numbers preceded by the letters COM or SEC or JOIN are Commission reference numbers.

Where only a Committee number is given, this usually indicates that no official text is available and the Government has submitted an "unnumbered Explanatory Memorandum" discussing what is likely to be included in the document or covering an unofficial text.

Abbreviations used in the headnotes and footnotes

AFSJ	Area of Freedom Security and Justice
CFSP	Common Foreign and Security Policy
CSDP	Common Security and Defence Policy
ECA	European Court of Auditors
ECB	European Central Bank
EEAS	European External Action Service
EM	Explanatory Memorandum (submitted by the Government to the Committee) *
EP	European Parliament
EU	European Union
JHA	Justice and Home Affairs
OJ	Official Journal of the European Communities
QMV	Qualified majority voting
SEM	Supplementary Explanatory Memorandum
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Euros

Where figures in euros have been converted to pounds sterling, this is normally at the market rate for the last working day of the previous month.

Further information

Documents recommended by the Committee for debate, together with the times of forthcoming debates (where known), are listed in the European Union Documents list, which is published in the House of Commons Vote Bundle each Monday, and is also available on the parliamentary website. Documents awaiting consideration by the Committee are listed in "Remaining Business": www.parliament.uk/escom. The website also contains the Committee's Reports.

*Explanatory Memoranda (EMs) and letters issued by the Ministers can be downloaded from the Cabinet Office website: http://europeanmemoranda.cabinetoffice.gov.uk/.

Staff

The current staff of the Committee are Ravi Abhayaratne (Committee Operations Assistant), Joanne Dee (Deputy Counsel for European and International Law), Alistair Dillon and Leigh Gibson (Senior Committee Specialists), Nat Ireton and Apostolos Kostoulas (Committee Operations Officers), Luanne Middleton (Second Clerk), Daniel Moeller (Committee Operations Manager), Jessica Mulley (Clerk), Foeke Noppert (Senior Committee Specialist), Indira Rao (Counsel for European and International Law), Paula Saunderson (Committee Operations Assistant), Emily Unwin (Deputy Counsel for European and International Law), Dr George Wilson (Second Clerk), Beatrice Woods (Committee Operations Officer).

Contacts

All correspondence should be addressed to the Clerk of the European Scrutiny Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is (020) 7219 3292/5467. The Committee's email address is escom@parliament.uk.

Contents

1 Cybersecurity: EU Strategy and revised Network and Information Systems Directive[1]

These EU documents are politically important because:

- the Government acknowledges that the final Network and Information Systems Directive has the potential to be raised with the UK by the EU under Article 13(4) of the Northern Ireland Protocol (which covers planned or adopted EU law that falls within the scope of the Protocol but which neither amend nor replace an EU act listed in the Annexes); and
- as the Communication refers to a cybersecurity framework that the UK has maintained after EU Exit, it holds domestic relevance for the Government as it develops the UK's post-Brexit cybersecurity strategy.

Action

- Write to the Minister requesting more information.
- Draw to the attention of the Digital, Culture Media and Sport Committee, the Home Affairs Committee, the Foreign Affairs Committee and the Defence Committee.

Overview

1.1 The two documents under scrutiny concern a Commission Communication on the EU's Cybersecurity Strategy for the Digital Decade and a related proposal for a Directive on measures for a high common level of cybersecurity across the EU.

Document (a) (41774)—Joint Communication: Cybersecurity Strategy for the Digital Decade

1.2 The EU's Cybersecurity Strategy for the Digital Decade was adopted on 16 December 2020. The document outlines the EU's proposals and forthcoming interventions to bolster Europe's collective resilience against cyber threats and safeguard citizens and businesses by ensuring trustworthy and reliable services and digital tools. The European Commission considers this as one of its top priorities.

1 Document (a)—JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the EU's Cybersecurity Strategy for the Digital Decade; Council and COM number: 14133/20 and JOIN(20) 18; Legal base: N/A; Government Department: Digital, Culture, Media and Sport; Devolved Administrations: Not consulted; ESC number: 41774. Document (b)—Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148; Council and COM number: 14150/20 + ADDs 1–6 and COM(20) 823; Legal base: Article 114 TFEU, QMV, ordinary legislative procedure; Government Department: Digital, Culture, Media and Sport; Devolved Administrations: Not consulted; ESC number: 41773.

1.3 The strategy sets out an ambition of reaching a combined investment of public and private funds of €4.5bn[2] in cybersecurity preparedness during the course of the next Multi-Annual Financial Framework (MFF) period (2021–27). The Commission states that it will support the cyber security strategy initiatives with investment through the next long-term EU budget, notably the Digital Europe Programme and Horizon Europe, as well as the Recovery Plan for Europe. Member States have been actively encouraged to make use of the EU Recovery and Resilience Facility to boost their cybersecurity capabilities and match EU-level investment.

1.4 The Strategy details forthcoming legislative proposals to address the cyber and physical resilience of critical national infrastructure and networks. These issues are addressed in the accompanying proposal for a revised Network and Information Systems Directive (document (b)), which covers both medium and large companies, and is based on assessments of how critical their functions are for economic activities and society. In addition, the Strategy details a proposal for a revised Critical Entities Resilience Directive, which broadens the scope of the 2008 European Critical Infrastructure Directive,[3] covering 10 sectors including: public administration; financial market infrastructures; health; drinking water; wastewater; energy; transport; banking; digital infrastructure; and space.

1.5 The Commission aims to implement the EU Cybersecurity Strategy in 2021 and, once the European Parliament and Council review and adopt the revised Network and Infrastructure Systems Directive and the Critical Entities Resilience Directive, Member States will be required to transpose the two Directives within 18 months of their entry into force. Under the Critical Entities Resilience Directive, Member States will be required to adopt a national strategy for securing the resilience of critical entities and to perform regular risk assessments. In addition to the two Directives, the Commission also aims to introduce a proposed Regulation for internet of things (IoT) devices[4] in 2021.

1.6 The EU Cybersecurity Strategy covers a number of other priority areas, grouping these within three categories. These categories are described below.

'Resilience, technological sovereignty and leadership'

1.7 This category outlines measures for ensuring that infrastructure, services and all internet-connected devices within the EU should be fundamentally secure by design, resilient to cyber threats, and more amenable to the mitigation of vulnerabilities once they are discovered. In addition to the Critical Entities Resilience Directive, the EU proposes building a European Cyber Shield[5] for the purpose of information sharing, monitoring, and analysis. The EU sets out proposals for establishing a highly-secure communications infrastructure, to be supported by secure and cost-efficient communications capabilities, with an initiative to develop and deploy new and more secure forms of encryption and to devise new ways of protecting critical communication and data assets.

2 Approximately £3.8bn at current prices.

3 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance).

4 The Internet of Things (IoT) describes the network of physical objects that are embedded with sensors, software and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

5 The European Cyber Shield is a planned network of Artificial Intelligence-enabled Security Operations Centres that will be capable of detecting signs of a cyberattack and enable preventative action before damage occurs.

1.8 The EU outlines proposals for ensuring technological sovereignty and secure devices. This includes an emphasis on securing internet of things devices through a new duty of care for connected device manufacturers to address software vulnerabilities, as well as the deletion of end-of-life sensitive data. Following this, the EU will use enforcement to ensure resilience of connected devices. The strategy additionally sets out an ambition for greater global internet security, encouraging Member States to adopt a domain name system resolution diversification strategy. In its ambitions for ensuring technological sovereignty, the Strategy sets out to establish a reinforced presence on the technology supply chain and to demonstrate leadership in digital technologies and cyber security across the digital supply chain. To support these activities, the Strategy emphasises the importance of building a more cyber-skilled EU workforce. This will include expanding efforts to upskill the current workforce as well as developing, attracting and retaining cybersecurity talent to help invest in world class research and innovation.

'Building operational capacity to prevent, deter and respond'

1.9 Within this category, the EU seeks to leverage the full implementation of regulatory tools, mobilisation and cooperation to enable systematic and comprehensive information sharing and cooperation against cyber incidents. A key initiative proposed for mitigating cyber threats is a Joint Cyber Unit, which would serve as a virtual and physical platform for cooperation for the different cyber security communities in the EU. The establishment of the Unit seeks to create a common space for multi-stakeholder groups to nurture structured cooperation, facilitate operational and technical cooperation, and to harness the potential of operational cooperation and mutual assistance within existing networks and communities. Another initiative under this 'prevent, deter and respond' category is an EU cyber diplomacy toolbox, which uses an array of measures, potentially restrictive, seeking to resolve international disputes by peaceful means. Although not explicitly stated, the measures outlined in this section of the Cybersecurity Strategy could, in theory, apply to both private organisations and state-sponsored actors which are viewed as a cybersecurity threat.

1.10 Additional priorities include initiatives for tackling cybercrime in conjunction with the EU's counter-terrorism agenda and the Security Union Strategy. This covers the scrutiny of electronic evidence and navigating encryption while preserving function in the maintenance of fundamental human rights. Furthermore, the strategy makes a commitment to significantly boost cyber defence capabilities ensuring that cyber security and cyber defence are further integrated into the wider security and defence agenda and encourages the development of state-of-the-art cyber defence capabilities, tying in with ambitions to establish greater EU technological sovereignty.

'Advancing a global and open cyberspace through increased cooperation'

1.11 This category relates to the EU's ambition of working with international partners to strengthen the rules-based global order, promote international security and stability in cyberspace, and protect human rights and fundamental freedoms online. The Strategy seeks to continue establishing EU leadership on standards, norms and frameworks in cyberspace while, additionally, highlighting cooperation with partners and the multi-stakeholder community as an ongoing key commitment.

Document (b) (41773)—Proposal for a revised Network and Information Systems Directive

1.12 The document under scrutiny—document (b)—is a proposal for a revision of the Network and Information Systems Directive (also known as the 'NIS' Directive).[6] The proposal is based on the results of a review of the current iteration of the Directive.

1.13 The NIS Directive entered into force in 2016. It places requirements on EU Member States to identify 'Operators of Essential Services' and ensure that they have appropriate and proportionate security measures in place to manage and mitigate any risks to their network and information systems, and to ensure the security of critical services that are important for the economy and wider society. This could, for example, require utilities suppliers to undertake a tailored cybersecurity risk assessment before putting in place appropriate measures of mitigation or providers of key digital services, such as search engines, cloud computing services or online marketplaces, having to comply with bolstered security and notification requirements. Currently, in the UK, operators of essential services covered by the domestic NIS Regulations are those in the energy, transport, water, digital infrastructure, and health sectors.

1.14 The proposal under scrutiny would repeal the current NIS Directive and make amendments to its general framework. As the UK is no longer an EU Member State, it will not have to implement the proposed Directive. However, as the proposal refers to a framework that the UK has maintained after EU Exit, it retains domestic relevance.

Main proposed changes

1.15 One of the most notable changes proposed to the NIS Directive is to its scope. The current Directive covers the energy, transport, banking, financial services, health, drinking water, and digital infrastructure sectors. Organisations in scope of these sectors are named operators of essential services and are subject to a proactive (ex-ante) regulatory regime across the EU. In addition to this, digital service providers (comprising online marketplaces, online search engines, and cloud computing services) are also subject to the NIS Directive in a reactive (ex-post) manner.

1.16 The proposal under scrutiny would expand the sectoral application of the NIS Directive by adding the wastewater, public administration, space, postal and courier services, waste management, the production and distribution of chemicals, food production, processing and distribution, and manufacturing sectors.

1.17 The proposal also makes a change regarding the regulatory approach to these sectors, moving away from the distinction between operators of "essential services" (ex-ante) and "digital service" providers (ex-post) in favour of a new distinction between "essential" services and "important" services.

1.18 Both groups of entities would be subject to the same risk management requirements and reporting obligations; only the regulatory approach differs. Micro and small entities are excluded from the scope of the proposal (as per its current iteration), with some notable exceptions on a Member State case-by-case basis.

6 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

1.19 The proposal aims to eliminate identification thresholds and would, therefore, envisage that any medium or large enterprises that operate in the sectors covered by the Directive would fall under the scope of the Directive. An exception to this rule would apply only in circumstances where a Member State deems that organisations have a key role for the economy or society.

1.20 The proposal makes a number of other recommendations and changes regarding the scope of organisations falling under the framework. It explicitly brings data centre services in scope as essential entities and identifies the importance of addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers, which is notably absent from the current Directive. It also recognises the importance of managed security service providers in areas such as incident response, penetration testing, security audits, and consultancy, and recommends increased diligence in their selection given their susceptibility to cyberattacks.

1.21 The new proposal would create a European Cyber Crises Liaison Organisation Network (EU-CyCLONe) composed of representatives of EU Member State crisis management authorities, the European Commission, and the European Union Agency for Cybersecurity (ENISA).[7] It would aid the management of large-scale incidents and crises while coordinating large-scale incident responses.

1.22 The Commission also proposes the establishment of a European vulnerability registry, where ENISA would have the responsibility to establish and maintain an appropriate information system, policies, and procedures with a view to enabling important and essential services and their suppliers to disclose and register vulnerabilities present in ICT services. It would also provide an opportunity for interested parties to access the information on vulnerabilities in the register. This is part of the new Commission's proposal to develop a framework for coordinated vulnerability disclosure.

1.23 The NIS Directive requires national competent authorities to develop strategies on the security of network and information systems. The proposal builds on that requirement, adding in explicit requirements that are not present in the current version. Notable additions include, among others, the requirement to have a national policy to address cyber security in supply chains and a coordinated vulnerability disclosure policy.

1.24 In addition, EU Member States would also be required, beyond the requirements of the Directive, to establish national cybersecurity crisis management frameworks, where objectives and modalities in the management of large-scale cybersecurity incidents are set out.

The Government's position

1.25 Parliamentary Under-Secretary of State at the Department for Digital, Culture, Media and Sport, Matt Warman MP, wrote to us by separate Explanatory Memoranda on the Commission's Communication and proposed Directive on 26 January 2021.

7 Commission Recommendation (EU) 2017/1584 on a coordinated response to large-scale cybersecurity incidents and crises.

Document (a)—Cybersecurity Strategy

1.26 The Minister explains that there are no legal or political issues relating to the Communication as it concerns a strategy published by the EU applying solely to its Member States. Neither does the Government foresee any issues arising from the Communication in relation to the Protocol on Ireland/Northern Ireland to the UK/EU Withdrawal Agreement. That said, as the Communication refers to a cybersecurity framework that the UK has maintained after EU Exit, it has some domestic relevance.

1.27 To this end, the Minister notes that responsibility for delivering the strategic objectives under the UK's own National Cyber Security Strategy (NCSS) are distributed across Government, given various Departmental interests and a need for a cross-cutting Government response to cybersecurity challenges that the UK faces. Key ministerial responsibilities relating to cybersecurity are as follows:

- The Minister for the Cabinet Office is responsible to Parliament for the NCSS and overseeing its £1.9bn budget.
- The Home Secretary has responsibility to counter cybercrime, as well as lead on cyber security response. The Home Secretary is also the designated Cabinet Office Briefing Room Chair (COBR) for high category cyber incidents.
- The Secretary of State for Digital, Culture, Media and Sport leads on digital matters, including the relevant growth, innovation and skills aspects of cyber security.
- The Defence Secretary has responsibility for the National Cyber Force (a joint endeavour between Defence and Intelligence agencies).
- The Foreign Secretary has statutory responsibility for GCHQ[8] and thus for the NCSC.

Document (b)—Proposed revision of the NIS Directive

1.28 As with the Communication under scrutiny, the Minister explains that there are no legal or political issues relating to the proposed Directive as the UK is no longer an EU Member State and, as such, it is not obliged to transpose the proposed Directive into domestic law. Furthermore, the Directive, which has yet to be adopted by the EU, does not raise any matters of vital national interest to the UK.

8 Government Communications Headquarters is the intelligence and security organisation responsible for providing signals intelligence and information assurance to the UK Government and the UK Armed Forces.

1.29 Once again, the Minister does not foresee any issues arising from the Directive in relation to the Protocol on Ireland/Northern Ireland to the UK/EU Withdrawal Agreement, however he acknowledges that the final proposal could potentially be raised with the UK by the EU under Article 13(4) of the Protocol.[9] As such, the Government commits to further monitoring of the proposal throughout its negotiation and adoption.

Potential implications for the UK

Document (a)—Cybersecurity Strategy

1.30 In his Explanatory Memorandum, the responsible Minister (Matt Warman MP) states that the UK's exit from the EU on 31 December 2020 means that the UK is not subject to the provisions of the European Cybersecurity Strategy nor involved in its delivery or implementation.

1.31 That said, the Minister notes that there are a number of key areas outlined in the Strategy which align with UK interests and ambitions in the cybersecurity field such as: working with international partners to strengthen the rules-based global order; promoting international security and stability in cyberspace; attracting and increasing the talent pipeline; and investing in innovative cyber solutions to improve cyber resilience across the economy. The Minister also notes that it will want to continue engagement with the EU regarding shared ambitions, goals and solutions on a number of global cyber security issues as the UK's own National Cyber Security Strategy is updated and published later this year. To this end, there could also be wider considerations that the Government should be mindful of as it develops the UK's NCSS vis-à-vis international partners. The UK currently enjoys close cooperation with Five Eyes partners and NATO allies in the field of cybersecurity and future Government action in this field should consider these ties and their ongoing importance to UK cybersecurity policy.

1.32 Furthermore, the Government states that it is in the UK's interest to see how the EU's new initiatives develop and to encourage the sharing of best practice and lessons learned from these new initiatives in the context of increasing threats both from hostile state actors and sophisticated cyber criminals. The Government notes that Part 4 of the UK/EU Trade & Cooperation Agreement includes provisions for cooperation in the field of cyber security, and that it will use this means of engagement to discuss EU activities and areas where UK/EU cooperation is of mutual benefit. These include, but are not limited to: deterrence; capacity building; and technical cooperation.

9 Article 13(4) of the Protocol states "Where the Union adopts a new act that falls within the scope of this Protocol, but which neither amends nor replaces a Union act listed in the Annexes to this Protocol, the Union shall inform the United Kingdom of the adoption of that act in the Joint Committee. Upon the request of the Union or the United Kingdom, the Joint Committee shall hold an exchange of views on the implications of the newly adopted act for the proper functioning of this Protocol, within 6 weeks after the request. As soon as reasonably practical after the Union has informed the United Kingdom in the Joint Committee, the Joint Committee shall either: (a) adopt a decision adding the newly adopted act to the relevant Annex to this Protocol; or (b) where an agreement on adding the newly adopted act to the relevant Annex to this Protocol cannot be reached, examine all further possibilities to maintain the good functioning of this Protocol and take any decision necessary to this effect. If the Joint Committee has not taken a decision referred to in the second subparagraph within a reasonable time, the Union shall be entitled, after giving notice to the United Kingdom, to take appropriate remedial measures. Such measures shall take effect at the earliest 6 months after the Union informed the United Kingdom in accordance with the first subparagraph, but in no event shall such measures take effect before the date on which the newly adopted act is implemented in the Union."

Document (b)—Proposal for a revised Network and Information Systems Directive

1.33 In his Explanatory Memorandum, the responsible Minister (Matt Warman MP) states that, as the proposal for a revised NIS Directive is still under negotiation and was not adopted during the Brexit Transition Period, the UK is not under any obligation to transpose it into domestic legislation. The Government notes, however, that the original transposition of the 2016 Directive was given effect to by the Network and Information Systems (NIS) Regulations 2018, which will remain on the UK statute book as retained EU law.

1.34 Furthermore, the Government states that the UK conducted its own review of the NIS Regulations in May 2020[10] and that various legislative amendments to implement its recommendations have already been made.[11] These include:

- extending the scope of NIS provisions relating to the sharing of information by enforcement authorities;
- putting in place measures for operators of essential services which have head office operations abroad to introduce procedures for nominating UK-based personnel to act on their behalf; and
- establishing provisions for the circumstances under which an individual or organisation identified as being an operator of essential services no longer believes they meet the designation criteria.

1.35 The Government also notes that it will consider proposals for the EU's new NIS Directive, amongst other evidence, in development of the UK's own objectives and priorities for cyber security legislation in the next iteration of the UK's National Cyber Security Strategy and future reviews planned for the NIS Regulations.

1.36 As regards to the position of the UK as a third-country to the EU, the Trade & Cooperation Agreement provides for future cooperation in the field of cyber security. This will enable both sides to work together where it is in their mutual interest through expert committees and bodies including, for example the European Union Agency for Cybersecurity (ENISA). Notably, the Trade and Cooperation Agreement stipulates that the UK may, upon invitation, participate in some of the activities of the NIS Cooperation Group in order to support the exchange of information with regard to exercises relating to security of network and information systems, best practices and capacity-building. These endeavours fall within a wider umbrella of cooperation on cyber issues, where the UK and EU will cooperate where it is of mutual interest, on a shared ambition to promote and protect an open, free, stable, peaceful, and secure cyberspace.

10 HM Government, 'Post-Implementation Review of the Network and Information Systems Regulations 2018' (May 2020).

11 The Network and Information Systems (Amendment and Transitional Provision etc.) Regulations 2020 (SI 2020 / 1245).

Action

1.37 We have written to the Minister requesting further information on the potential implications of the EU's Cybersecurity Strategy for UK law and policy, in particular, concerning Northern Ireland, and UK-based stakeholders.

1.38 We have drawn this Report chapter to the attention of the Digital, Culture, Media and Sport Committee, the Home Affairs Committee, the Foreign Affairs Committee, and the Defence Committee.

Letter to the Parliamentary Under-Secretary at the Department for Digital, Culture, Media and Sport (Matt Warman MP)

The Committee has asked me to thank you for your two Explanatory Memoranda (EM) on the above listed documents.

In light of the end of the post-Brexit Transition Period—as per the UK/EU Withdrawal Agreement—and the recent agreement and provisional application of the UK/EU Trade and Cooperation Agreement (TCA), the Committee would appreciate it if you could provide further information on the following points.

- In the Government's EM on the Commission's proposed Directive, it was noted that elements of the legislation could potentially be raised with the UK by the EU under Article 13(4) of the Northern Ireland Protocol. Could you provide the Committee with further information on the likelihood of this transpiring and, were it to, what impact this could have on Government policy for the UK's own cybersecurity strategy?

- Part 4 of the TCA provides scope for future cooperation between the UK and the EU in the cybersecurity field. In light of this, could you provide the Committee with more information on how the UK might potentially interact with new and existing bodies outlined in the EU's Cybersecurity Strategy, such as its NIS Cooperation Group and Joint Cyber Unit, as well as the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) and the EU Agency for Cybersecurity (ENISA)?

- Depending on the nature of this interaction, could you provide the Committee with more information on what impact, if any, it will have on continued UK participation in the Five Eyes intelligence alliance and ongoing cooperation with NATO allies in the field of cybersecurity?

We request a response to this letter within 15 working days.

2 Data adequacy[12]

These EU documents have not been deposited by the Government under the current interim scrutiny arrangements. These documents are, however, legally and politically important because:

- once adopted, they will provide the EU legal basis for the transfer of personal data from the EU to the UK. This is vital for the conduct of trade and law enforcement cooperation under the UK/EU Trade and Cooperation Agreement (TCA);

- there are still stages in the adoption process which could delay the date of their adoption. In particular, any amendments which the Commission may need to make in response to the opinion of the European Data Protection Board, expected in April. This could present the risk of a data flows "cliff-edge" for the UK, as the bridging provisions under the Trade and Cooperation Agreement would only allow personal data flows to continue to the UK from the EU until the end of June at the latest;

- after adoption, they will be under constant review and monitoring by the EU Commission as to whether the UK continues to provide "essentially equivalent" data protection and open to legal challenge in the EU legal order. Unless extended, they will in any event expire after 4 years. Any cessation in their application could be disruptive of both trade and law enforcement under the TCA; and

- effective Parliamentary scrutiny of the maintenance of adopted decisions and the corresponding UK data protection legal framework forms one of the grounds on which the Commission has made its provisional positive data adequacy assessment for the UK. The Government also relied on effective scrutiny as a control on the Executive in its own "Adequacy Framework" to the Commission in March 2020. It will therefore be vital to the continuing application of the adopted decisions that the Government facilitate in a meaningful way the scrutiny of the House, this Committee and other interested Departmental Select Committees.

12 (a) Proposal for a Commission Implementing Decision;—; Article 45(3) of Regulation 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) ; DCMS;—; 41796; (b) Proposal for a Commission Implementing Decision;—; Article 36(3) of Directive 2016/680 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data and repealing Council Framework Decision 2008/977 JHA; HO;—; 41797.

Action

- To write to the Government for their initial view and response to our specific questions.
- To report to the House and draw these matters to the attention of International Trade Committee; the Home Affairs Committee; the Digital, Culture, Media and Sport Committee; the Business and Industrial Strategy Committee; the Science and Technology Committee; the Health and Social Care Committee; the Northern Ireland Affairs Committee and the Joint Committee on Human Rights.

Overview

2.1 A data adequacy decision that a third country provides "essentially equivalent" personal data protection to the EU comprises the most comprehensive and seamless basis for the transfer of data from the EU to that country. Whether for the purpose of trade or cooperation on law enforcement, data adequacy decisions enable data to flow lawfully to third countries from the EU without the need for further safeguards.

2.2 The flow of personal data from the EU to the UK is vital for the EU-UK future relationship, particularly in terms of trade and law enforcement cooperation under the UK/EU Trade and Cooperation Agreement (TCA).

2.3 On Friday 19 February, the EU Commission published both:

- a draft Commission Implementing Decision for processing of personal data for commercial purposes based on the General Data Protection Regulation[13] (GDPR); and
- a draft Commission Implementing Decision for processing based on the Law Enforcement Data Protection Directive[14] (LED).

Further background information

2.4 The Government had hoped that data adequacy decisions would be in place before the end of the transition period, having already itself legislated to allow UK to EU data flows. As they were not in place, the Trade and Cooperation Agreement (TCA) included "bridging provisions" to enable data flows from the EU to the UK to continue as they did before the end of the transition period, until 30 April 2021. These can be extended to 30 June 2021 at the latest. Quick progress towards adoption before the expiry of the "bridging provisions" is clearly desirable.

13 Article 45 (3) of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

14 Article 36(3) of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

2.5 Obtaining data adequacy decisions in these areas has therefore been an important goal for the Government. They published their formal application to the EU for adequacy decisions on 13 March 2020.

2.6 Our initial assessment of the Government position has been drawn from:

- the Press Release the Government published on 19 February following the Commission's publication of the draft decisions; and
- reports in the media (for example, an article on data and the Government's new approach to data published in the Financial Times (FT) on 27 February by the Secretary of State for Digital, Culture, Media and Sport (The Rt Hon. Oliver Dowden CBE MP)).[15]

2.7 We address the political and legal importance of these documents and the need for their effective Parliamentary scrutiny later in this chapter (see both "Our Assessment" and our letter to the Government).

Our Assessment

Scrutiny of these documents

2.8 Following the end of the post-Brexit transition period, the Government agreed to deposit documents relating to the Northern Ireland Protocol[16] but no other EU documents are currently being deposited. These are the interim arrangements under which EU document scrutiny is presently taking place until the Government and the House reach a new arrangement.

2.9 The EU documents considered in this chapter have not been formally deposited by the Government and therefore we have not received an Explanatory Memorandum outlining their potential implications for UK law and policy.

2.10 This Committee's remit is still to report to the House on EU documents of political and legal importance. This has not changed since 1 January 2021.

2.11 The political importance of these documents is clear given their centrality to both trade and law enforcement cooperation between the EU and the UK.

2.12 While the documents once adopted will not be directly legally-binding on the UK,[17] nevertheless they have indirect legal or quasi-legal implications for the UK:

- if they cease to apply, then not only will this impede the flow of data from the EU to the UK for trade purposes but it could lead to suspension of parts or the whole of the Law Enforcement part of the TCA;[18]

15 "New approach to data is a great opportunity for the UK post-Brexit", 27 February 2021, Secretary of State for Digital, Culture, Media and Sport (Rt Hon. Oliver Dowden CBE MP).

16 Letter from Rt Hon Michael Gove (Chancellor of the Duchy of Lancaster) to Lord Kinnoull Lords EU Committee, 14 January 2021

17 They are only binding in the EU internal legal order and are addressed to the Commission and Member States.

18 If due to "serious and systemic" failures in data protection on the part of the UK.

- they contain text which is addressed to the UK and seems to create important expectations for the maintenance of the decisions—Recitals 275 of the GDPR decision and 165 of the LED decision note the ongoing monitoring obligations of the Commission of UK adequacy and state: "To this end, the UK authorities are invited to inform the Commission of any material change to the UK legal order that has an impact on the legal framework that is the object of this Decision…";
- they may also have a constraining effect in the sense that should the UK stray too far from the bases for the Commission's positive adequacy assessment set out in the Recitals to the decisions, then may lead or contribute to the decisions being withdrawn or suspended; and
- this in turn may reduce the Government's latitude for amending its current, EU-based data protection legislative framework.

2.13 Most telling of all, effective Parliamentary oversight of data protection issues by the Home Affairs Committee is referred to in the draft GDPR data adequacy decision[19] as a contributing factor to the Commission's overall adequacy assessment. The Government itself relies[20] on this oversight in its submission documents to the EU.

2.14 It is also relevant that the Chancellor of the Duchy of Lancaster (Rt Hon. Michael Gove MP) recently recognised the breadth and importance of this Committee's responsibilities as now the sole Committee in the House of Commons with a specific EU scrutiny remit. In giving evidence[21] to us on 8 February, he made reference to the Committee on the Future Relationship of the EU which ceased to exist on 16 January. He added:

> That means inevitably that this Committee takes on even more responsibilities. Ultimately I don't think its the Government that should decide the shape or the agenda of Select Committees; that is a House matter, but of course we will do everything we can to facilitate the effective scrutiny that the House needs to enjoy of Government activity.

2.15 In summary, these are important and lengthy documents, with detailed recitals (87 and 49 pages respectively). Effective Parliament scrutiny of the Government's activity and policy in relation to the decisions and the data protection framework forms a ground for the Commission' positive adequacy assessment which the Government would be wise then to facilitate in a meaningful way. They are therefore deserving of our further scrutiny, informed by an official view from the Government and a prompt and full response to our specific questions set out in our letter.

Potential challenges for the Government

Before the adoption of the decisions

2.16 As the adoption of the decisions is a unilateral EU process, the Government can only urge the EU to complete the process swiftly.

19 See recital 3.2.3.4.

20 See "Select Committees" heading, page 44 of Section F Law Enforcement, UK Government's "Adequacy Framework".

21 Q6, Oral evidence: The UK's new relationship with the EU, HC 1197, 8 February 2021.

2.17 While the publication of the draft decisions is proof that the Commission itself considers that the UK currently provides "essentially equivalent" data protection to the EU, it only marks the start of the decision-making process for their adoption. Further stages still to be navigated. In particular the adoption process could be delayed if the European Data Protection Board (EDPB) takes issue with the draft decisions and the Commission needs to amend them. While the EDPB discussed the draft decisions at its recent meeting of 9 March,[22] at the time of writing there is no official confirmation of when the opinion may be delivered. Media expectation is that the opinion will be published in mid-April.[23] However, there is no fixed timetable for the overall adoption process involving a committee of expert representatives from the Member States.

After adoption

2.18 Even after adoption, there are other potential challenges for the Government to navigate:

- The current drafts provide for the decisions to expire in 4 years' time, unless extended.
- Even before then, the Commission is under an ongoing obligation to keep the decisions under review and to amend, suspend or revoke the decisions at any time should it consider that the UK no longer provides equivalent protection.
- Although the European Parliament has no formal role in the adoption process, it can prompt the Commission to undertake a review of the decisions and its LIBE Committee has voiced concerns about use of data by UK intelligence bodies.
- There will be scope for the validity of the decisions to be challenged before the Court of Justice (CJEU), just like previous US adequacy decisions in Schrems 1[24] (Safe Harbour) and Schrems 2[25] (Privacy Shield). The access to personal data by intelligence and security services has become a particularly sensitive area and bulk, indiscriminate access has been ruled incompatible with EU law (see also in the context of the e Privacy Directive,[26] the CJEU ruling in Privacy International).[27]
- If either decision ceases to apply, this could have consequences under the TCA: if due to "serious and systemic" failures in data protection this could lead to suspension of Law Enforcement cooperation, in whole or part.[28]

22 The EDPB Press Release of 10 March states "The Board discussed the draft UK adequacy decisions, which were received from the European Commission. The EDPB will thoroughly review the draft decisions, taking into account the importance of guaranteeing the continuity and high level of protection for data transfers from the EU".

23 See MLex headline "UK data adequacy decisions due to receive EDPB opinion in mid-April" (26 February 2021). Viewing the full article requires a subscription.

24 C-362/14.

25 C-311/18.

26 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

27 C623–17.

28 See Art.LAW.OTHER.137 TCA.

- Again, if either decision ceased to apply, reliance would have to be placed on alternative mechanisms under the GDPR and LED. In the case of the GDPR, a next best option of "standard contractual clauses" (SCCs) is not attractive since the utility of these has been undermined by the Schrems 2 ruling. Until the Commission formally adopts its new draft SCCs, data exporters relying on SCCs are required by the CJEU's ruling to carry out mini adequacy assessments of their own as to the protection offered by the country of destination

2.19 The Government will need to bear all these "post-adoption" factors listed in mind, when deciding to diverge from EU data protection law in future. Some future divergence seems likely, as indicated by the Secretary of State's article in the FT (see paragraph 0.6 above) and further media reports.[29] We also note that the consultation on the Government's National Data Strategy ended on 9 December 2020. There is nothing in those reports to indicate that any changes are imminent or would pre-empt any adoption process. However, the Government's position might be clearer if the Minister were to address Parliament or to write to this Committee directly on this issue (see the letter to the Government at the end of this chapter).

2.20 Maintaining the adequacy decisions, once adopted, also relies on the Government recalling the broader range of factors that the EU Commission must consider when monitoring and reviewing the decisions. This means that changes not only to the UK data protection legal framework, but also wider legal and constitutional changes could have an impact. Specifically, those relating to the "rule of law" or "respect for human rights". Likewise, how legal obligations under relevant international agreements between the EU and UK (including the Withdrawal Agreement and the Trade and Cooperation Agreement) but also between UK and other countries are interpreted and applied by the UK.

Action

2.21 We have written to the Government in the terms set out below, asking for its view of the documents and focussing on these areas:

- How the Government will assess and manage the risk to the maintenance of the adequacy decisions should it wish to diverge from EU data protection law in future.
- What arrangements there will be for monitoring EU developments that could cause divergence between the EU and UK legal frameworks in this area, both in terms of new data protection legislation and CJEU case law.
- How the Government will ensure that its own new adequacy assessments for non-EU countries do not cause "equivalence" difficulties in terms of onwards transfer from the UK to those countries of personal data originating from the EU.
- The same question for any international agreements between the UK and non-EU countries which involve data exchange.

29 For example, Sky News, 'Government to reform data protection laws to spur economic growth' (11 March 2021)

- What arrangements there will be for communication between the EU, UK Government and the Information Commissioner on matters potentially affecting the maintenance of the adequacy decisions.
- To what extent the Government will need to take a different or enhanced approach to maintaining the Law Enforcement data adequacy decision.
- How the Government proposes to keep Parliament and this Committee informed on these matters on a regular, timely, responsive and transparent basis, particularly in the lead-up to the four-year expiry/extension deadline.

2.22 The draft decisions are of cross-cutting relevance to the work of many Committees across the House. We are therefore also drawing the documents and this Report chapter to the attention of International Trade Committee; the Home Affairs Committee; Digital, Culture, Media and Sport Committee; the Business and Industrial Strategy Committee; the Science and Technology Committee; the Health and Social Care Committee; the Northern Ireland Affairs Committee and the Joint Committee on Human Rights.

Letter from the Chair to the Minister for Media and Data (Rt Hon. John Whittingdale OBE MP), Department for Digital, Culture, Media and Sport and the Parliamentary Under-Secretary of State (Kevin Foster MP), Home Office

The Committee has asked me to write to you concerning the draft data adequacy decisions that the EU Commission published on 19 February 2021. As one relates to the flow of personal data to the UK from the EU for commercial purposes and the other for law enforcement purposes, we thought that our scrutiny of the documents would involve both of your respective Ministerial remits.

You may be aware that following the end of the post-Brexit transition period, the Government agreed to deposit documents relating to the Northern Ireland Protocol but no other EU documents are currently being deposited. These are the interim arrangements under which EU document scrutiny is presently taking place until the Government and the House reach a new arrangement.

The draft EU data adequacy decisions have not been formally deposited by the Government and therefore we have not received an Explanatory Memorandum outlining their potential implications for UK law and policy. We consider these documents to be of significant legal and political importance and have a number of questions regarding their potential implications for the UK.

When preparing your response to the Committee, you may wish to bear in mind that effective Parliamentary scrutiny of the Government's data protection activities forms one of the grounds on which the Commission has made its initial positive data adequacy assessment. Effective Parliamentary oversight of data protection issues by the Home Affairs Committee is referred to in the draft GDPR data adequacy decision.[30] The Government

30 See recital 3.2.3.4.

itself relies[31] on this oversight in its submission documents to the EU. It is therefore important for the adoption and maintenance of these decisions that Government does all it can to facilitate in a meaningful way both ours and other Select Committee scrutiny.

As you know, these draft decisions are not yet 'done and dusted'. There are still some potential hurdles in the adoption process, including the opinion of the European Data Protection Board. We understand from media reports that the opinion in expected in mid-April. We would be grateful if you could update our officials as to whether that timetable is accurate and indeed as to any other indications of the likely timetable for adoption of the decisions. In any event, we would expect you to inform the Committee of any likely sticking points that emerge in the opinion and what the Government can do in response to provide any reassurance to the Commission. We are mindful of the risks of any delays to the adoption process, given that the current bridging arrangements for continued EU to UK data flows only last until the end of June at the latest.

Assuming that the decisions are adopted in time, we have a number of questions as to how the Government will ensure in future that the decisions remain in place and are extended beyond their four-year shelf life. We are aware of the potential for both the Commission to amend, suspend or revoke the decisions should it consider that the UK no longer provides "essentially equivalent" data protection to the EU. We are also aware of the potential for legal challenge of the decisions before the Court of Justice (CJEU) given the fate of both US data adequacy decisions. We also note the potential problems that could be caused for both the good functioning of the trade and law enforcement parts of the Trade and Cooperation Agreement (TCA) should the decisions run into difficulty. In view of these risks, we would like to know:

- How will the Government assess and manage the risk to the maintenance of the adequacy decisions should it wish to diverge from EU data protection law in future? Divergence seems likely to us, in the light of the article in the Financial Times (FT) written by the Secretary of State for Digital, Culture, Media and Sport (The Rt Hon. Oliver Dowden CBE MP) on 27 February, though the timing and extent is less clear.

- Linked to this, how does the Government propose to approach the "invitation" in Recitals 275 of the GDPR decision and 165 of the LED decision which note the ongoing monitoring obligations of the Commission of UK adequacy and state: "To this end, the UK authorities are invited to inform the Commission of any material change to the UK legal order that has an impact on the legal framework that is the object of this Decision…". What would it consider to be a "material change" and how wide does it consider the relevant "legal framework" to be? Would that encompass any material future changes the Government may wish to make in due course to judicial review or the Human Rights Act? How will Parliamentary scrutiny be included in that process? Will Parliament be informed at the same time as the EU Commission?

- What arrangements will there be in Government for monitoring EU developments that could cause divergence between the EU and UK legal frameworks in this

31 See "Select Committees" heading, page 44 of Section F Law Enforcement, UK Government's "Adequacy Framework".

area, both in terms of new data protection legislation and CJEU case law? How will dialogue take place between the EU and the UK about managing such divergence? How will Parliamentary scrutiny be included in that dialogue?

- How will the Government ensure that its own new adequacy assessments for non-EU countries do not cause "equivalence" difficulties in terms of onwards transfer from the UK to those countries of personal data originating from the EU? We note in this respect from the Secretary of State's FT article that the Government is keen to adopt significantly more adequacy assessments for non-EU countries than the EU currently has.
- How will the Government ensure that "equivalence difficulties" are not caused by data protection, data exchange and digital trade provisions in any international agreements between the UK and non-EU countries?
- What arrangements, if any, will there be for communication between the EU, UK Government and the Information Commissioner on matters potentially affecting the maintenance of the adequacy decisions?
- To what extent, if any, will the Government need to take a different or enhanced approach to maintaining the Law Enforcement data adequacy decision?
- How does the Government interpret the ART.LAW.OTHER 137 in terms of possible suspension of parts or the whole of Part 3 Law Enforcement Cooperation of the TCA? If one or either of the two adequacy decisions ceased to apply, would that be sufficient for one party to suspend obligations or it is beyond doubt that the "serious and systemic deficiencies" as regards the relevant party's data protection would also need to be established?
- How does the Government propose to keep Parliament and this Committee informed on these matters on a regular, timely, responsive and transparent basis, particularly in the lead-up to the four-year expiry/extension deadline?

2.23 We look forward to receiving a response to this letter within 10 working days.

3 Northern Ireland Protocol: Market access for goods from African, Caribbean and Pacific (ACP) countries[32]

This EU document is legally and politically important because:

- it concerns the EU's Market Access Regulation which sets out the arrangements for goods originating in some African, Caribbean and Pacific countries to access the EU market;
- the Market Access Regulation continues to apply in Northern Ireland under Article 5 of the Protocol on Ireland/Northern Ireland;
- the Withdrawal Agreement Joint Committee has established criteria for determining whether goods brought into Northern Ireland are "at risk" of entering the EU market and must be charged the applicable EU tariff; and
- goods that are subject to EU safeguard measures (such as a higher tariff or quota) under the Market Access Regulation are likely to be considered "at risk" and charged the higher EU tariff if they enter the UK via the Northern Ireland.

Action

- Draw to the attention of the Northern Ireland Affairs Committee, the International Trade Committee, and the International Development Committee.

Overview

3.1 This European Commission report concerns the operation of the EU's Market Access Regulation (2016/1076) which sets out market access arrangements for goods originating in certain African, Caribbean and Pacific (ACP) countries.[33] The arrangements apply in the period between the conclusion of negotiations on an Economic Partnership Agreement (EPA) with the EU and its ratification and entry into force. EPAs are trade and development agreements. Their purpose is to encourage sustainable development and poverty reduction in ACP countries through preferential (duty- and quota-free) access to the EU market. The Market Access Regulation provides a bridge to these preferential terms. It gives the European Commission power to amend the list of ACP countries to whom the market access arrangements apply (for example, by removing a country if it has failed to ratify an EPA within a reasonable period of time) and to make other technical changes. It also

32 European Commission report on the exercise of delegated powers under Regulation (EU) 2016/1076; Council document 5253/20, COM(20) 7; Legal base—; Dept—International Trade; Devolved Administrations—not consulted; ESC number 41031.

33 See Regulation (EU) 2016/1076 applying the arrangements for products originating in certain states which are part of the African, Caribbean and Pacific (ACP) Group of States provided for in agreements establishing, or leading to the establishment of, economic partnership agreements.

allows the EU unilaterally to impose safeguard measures—essentially customs duties or tariff quotas—if there is a surge in imports which might cause serious injury to domestic industry in the EU, to sectors of the economy, or to agricultural markets.

3.2 The Market Access Regulation forms part of the body of EU law that continues to apply in Northern Ireland, but not the rest of the UK, under the Northern Ireland Protocol.[34] In earlier correspondence, the Minister of State at the Department for International Trade (Rt Hon. Greg Hands MP) told us that the Government saw no need to replicate in domestic law the unilateral safeguard provisions contained in the Regulation.[35] He added that the 2016 Regulation would only 'bite' on "at risk" goods—in this case, ACP goods brought into Northern Ireland which were considered to be "at risk" of onward movement to the EU.

3.3 While the Minister was unable to speculate on the outcome of discussions in the Withdrawal Agreement Joint Committee on the criteria for determining "at risk" goods and how these criteria would affect the application of EU tariff and quota-based safeguards on goods entering Northern Ireland, he made clear that even where goods were classified as 'at risk' of entering the EU market, the Government intended to "make full use of the provisions in the Protocol to waive and/ or reimburse higher tariffs where these have been paid". The Minister also highlighted the Government's Trader Support Service (TSS) which was established to provide free "end-to-end support for traders importing into Northern Ireland" and to "avoid burdening businesses with any potential complexities in the system—including any associated with the 'at risk' regime".[36]

3.4 We wrote to the Minister in December asking him to update us on any agreement reached in the Withdrawal Agreement Joint Committee on the criteria for determining "at risk" goods and to explain how these criteria would affect the application of EU tariff and quota-based safeguards imposed under the Market Access Regulation on goods entering Northern Ireland.[37]

3.5 In his response of 12 February 2021, the Minister says that Joint Committee Decision No 4/2020 (agreed on 17 December 2020) establishes the relevant "at risk" criteria and that "EU tariffs will only be charged where goods are destined for the EU, or where there is a genuine risk of onward movement". He continues:

> Businesses authorised under the UK Trader Scheme can undertake that the goods they are moving into Northern Ireland are 'not at risk' of onward movement to the EU. These goods will therefore not be liable to EU tariffs. To avoid shell or letterbox businesses from taking advantage of this scheme, the UK Trader Scheme will be open only to businesses established in Northern Ireland, or businesses who meet certain closely linked criteria. For imports into NI from outside the UK or the EU, the scheme will apply where the differential between the UK and EU's tariffs is less than 3% points.

34 See Article 5(4) and Annex 2 of the Protocol on Ireland/Northern Ireland.

35 See our letter of 23 April 2020 and the letter of 6 May 2020 from the Minister for State at the Department for International Trade (Rt Hon. Greg Hands MP) to the Chair of the European Scrutiny Committee (Sir William Cash MP).

36 See the Minister's letter of 25 November 2020 to the Chair of the European Scrutiny Committee (Sir William Cash MP).

37 See our letter dated 9 December 2020 to the Minister of State (Rt Hon Greg Hands MP) at the Department for International Trade.

Our assessment

3.6 Under the relevant provisions of the Northern Ireland Protocol, traders must establish that the goods they bring into Northern Ireland from outside the UK and the EU are "not at risk" of subsequently being moved into the EU, applying the criteria set out in Joint Committee Decision No 4/2020 on the determination of goods not at risk. Two sets of criteria are relevant in the case of goods which are brought into Northern Ireland directly from ACP countries. These goods will be considered "not at risk" and, as such, will not be charged an EU tariff if:

- they are not subject to commercial processing in Northern Ireland and the applicable UK tariff is equal to or higher than the applicable EU tariff; or
- they are not subject to commercial processing in Northern Ireland and the goods are brought in by an authorised trader under the UK Trader Scheme and the difference between the applicable EU and UK tariff is less than 3% of the customs value of the goods.

3.7 Conversely, if by applying these criteria the goods are considered to be at risk, then different tariff quotas or customs duties could apply to the same goods, depending on their point of entry into the UK—the EU tariff for entry via Northern Ireland and the UK tariff for entry via Great Britain. Goods which are subject to safeguard measures under the Market Access Regulation are far more likely to attract a higher EU tariff. This is because the Joint Committee Decision disapplies the second set of criteria for goods subject to EU trade defence measures—and safeguard measures under the Market Access Regulation are a form of trade defence—meaning that they are less likely to meet the criteria for "not at risk" goods.

3.8 The Minister does not reiterate the commitment given in his earlier letter of 25 November 2020 to "make full use of the provisions in the Protocol to waive and/ or reimburse higher tariffs where these have been paid" and to "minimise the impact on Northern Ireland business and traders as a result of the Protocol". We trust that it nonetheless still stands.

Action

3.9 We draw our observations and correspondence with the Government to the attention of the Northern Ireland Affairs Committee, the International Trade Committee, and the International Development Committee.

4 Public country-by-country tax reporting of multinationals in the EU[38]

This EU document is politically important because:

- it would require large multinationals with operations in the EU to publish country-by-country (CbC) reports on where they pay tax for public scrutiny. After more than four years of negotiations, a majority of the EU's remaining 27 Member States in February 2021 provisionally endorsed the principle of such public CbC reporting under EU law, and negotiations are currently on-going on the final text of the legislation; and
- although the Government has repeatedly said it would consider introducing CbC tax reporting requirements for large companies under UK law on a multilateral basis, it is unclear if Ministers would be willing to take that step in tandem with the EU—especially given the current political tensions in the UK/EU relationship—should the latter formally require all its Member States to make such disclosures mandatory.

Action

- Write to the Financial Secretary to the Treasury (Rt Hon. Steve Barclay MP) to request further information on the Government's views on the EU's efforts to introduce public country-by-country tax reporting for multinationals.
- Draw these developments to the attention of the Business, Energy and Industrial Strategy Committee, the Public Accounts Committee and the Treasury Committee.

Overview

4.1 One of the measures[39] being considered within the European Union to tackle aggressive tax avoidance by large multinational companies is to make them subject to mandatory public "country-by-country" (CbC) reporting, which would show in which tax jurisdictions they are recording their profits and in which ones they are paying tax (and how much). The—untested—logic is that increased public scrutiny of their tax affairs will put pressure on such companies to reduce their reliance on tax avoidance arrangements.

38 Proposal for a DIRECTIVE amending Directive 2013/34/EU as regards disclosure of income tax information by certain undertakings and branches; Council number 7949/16, COM(16) 198; Legal base: Article 50(1); ordinary legislative procedure; QMV; Department: HM Treasury; Devolved Administrations: Not consulted; ESC number: 37663.

39 The proposed introduction of public CbC reporting requirements for multinationals is only one of various measures being pursued at EU-level (and internationally) to address tax avoidance and evasion. For example, separate discussions are on-going about the taxation of the digital economy, where base erosion and profit shifting is especially pronounced, and the EU recently announced that it would try to establish a joint approach with the United States on this issue. The European Commission is also due to publish an "Action Plan" on EU corporate taxation policy later in 2021.

4.2 The European Commission tabled draft legislation in early 2016 to introduce public CbC requirements under the EU's Accounting Directive for the largest companies with operations in the EU. However, some countries have warned that forcing companies headquartered in the EU to make such disclosures, which their competitors elsewhere in the world would not be subject to (or only in relation to their branches and subsidiaries within the EU), could affect their competitiveness.[40] These concerns have led several countries—notably Ireland—to object to the legal basis chosen by the Commission for its proposal. They argue that the new Directive is a tax measure rather than accounting policy, which would mean every EU Member State could veto the draft legislation.[41] However, several EU countries that were initially opposed have changed their position, and in early 2021 a "clear majority" of Member States provisionally endorsed the proposal despite these concerns. The European Parliament—which must also give its approval to the legislation—is also supportive.

4.3 Negotiations on the final text of the Directive are still on-going, so it is unclear when the new CbC reporting requirement may take effect within the EU, or what its precise substance will be. Concerns over the appropriate legal base for the legislation could also render the future legislation vulnerable to legal challenge before the EU Court of Justice.

4.4 The Government was supportive of the proposal while the UK was a Member State, but its views on the merits of the Directive now that the UK has left the EU are unclear. In particular, although Ministers have said repeatedly they would be willing to introduce public CbC reporting under UK law as part of a multilateral effort (to avoid harming competitiveness by doing so unilaterally), they have not indicated whether the introduction of such disclosures in all 27 EU countries simultaneously would allow the UK to follow suit.

4.5 In the remainder of this chapter we have further explored the draft EU Directive on public country-by-country reporting and its possible implications for UK policy in this area.

Public country-by-country tax reporting

4.6 In the field of tax policy, a key concern of policy-makers is that large multinational enterprises (MNEs) are able to exploit the gaps and mismatches between the tax rules of different countries. They can use these differences to artificially eliminate their profits, or shift them to low or no-tax jurisdictions where there is little or no economic activity, resulting in little or no overall corporate tax being paid. To address problems associated with "base erosion and profit shifting" (BEPS)—in particular the impact on tax revenues and hence the ability of governments to spend—the Organisation for Economic Co-operation and Development (OECD) published an Action Plan in 2015. One of the many proposed measures concerned so-called country-by-country (CbC) reporting by MNEs, to provide tax authorities with more information on where such companies pay their tax.

40 The fact that the envisaged disclosures might also show certain EU countries accounting for a share of corporation tax paid by Multinational Enterprises disproportionate to the size of their domestic market is also likely to cause concern.

41 The draft Directive as tabled is based on Article 50 TFEU, which allows the EU to set company law, rather than Article 115 TFEU, which covers EU tax policy such as corporate tax. The crucial difference is that new rules under Article 50 only needs the support of a Qualified Majority of Member States in the EU's Council of Ministers, whereas Article 50 legislation requires unanimity, giving each country a veto.

4.7 In the EU (and, at the time, the UK) this was implemented by means of a 2016 Directive that sets out the types of country-by-country tax information that all Member States must collect from companies operating in their territory, and how this data is shared with the tax authorities of other EU countries. However, the information required under that piece of legislation—in line with the recommendations made by the OECD—is solely provided to tax authorities, and treated confidentially. Data on where companies pay corporation tax is not generally required to be made available for public scrutiny, although the EU's banking, extractive and logging industries[42] are already subject to a sector-specific requirement to disclose publicly where they pay tax.

4.8 In April 2016, in the aftermath of the Panama Papers tax evasion scandal, the European Commission tabled further draft EU legislation that would require large MNEs to make their CbC tax information public. The logic behind requiring disclosure of such information by these companies is that the increased scrutiny of whether they are paying tax where they earn their profits would put pressure on them to reduce their reliance on convoluted tax arrangements. As a new approach, the effectiveness of public country-by-country reporting in that respect is not proven.

4.9 The substance of the Commission proposal, and the current state of play in the negotiations on its adoption, are discussed further below.

The draft EU Directive on disclosure of country-by-country tax reports

4.10 The draft legislation tabled by the European Commission in spring 2016 would amend the EU Accounting Directive—which governs corporate reporting—to impose a public country-by-country reporting requirement on all large EU headquartered MNEs and non-EU headquartered MNEs operating in the EU, where they have a total consolidated annual group revenue above €750 million (£648 million).[43]

4.11 More specifically, this CbC Reporting Directive would require such multinational companies to publish annual tax reports on their website describing, among other things, their net turnover; profits or losses before tax; and the amount of corporation tax due and already paid. Underlining the ultimate purpose of the Directive, this information would need to be broken down for each EU Member State in which the company operates, and similarly for each non-EU jurisdiction deemed "not comply with good governance standards in taxation" (a euphemism for non-EU tax havens). The European Commission had suggested that it should have the power to establish a list of such tax havens by means of a Delegated Act, a type of EU Statutory Instrument (which would, confusingly, be separate from the existing EU list of "non-cooperative tax jurisdictions" that is agreed biannually by EU Finance Ministers).[44] For all other jurisdictions, namely non-EU countries considered to have adequate tax governance standards, the country-by-country data would need to be reported only on an aggregated basis.

42 Article 89 of the Capital Requirements Directive (Directive 2013/36/EU) and Article 44 of the Accounting Directive (Directive 2013/34/EU).

43 This is the OECD threshold in its CbC model, which it estimates—if rolled out globally—would cover MNEs controlling around 90% of corporate revenues, whilst excluding 85–90% of MNEs from the requirements.

44 Under the proposed Directive, non-EU countries could be blacklisted for example in relation to their refusal to exchange information on taxpayers or their alleged unfair tax practices.

4.12 One of the key issues is how the new reporting requirements would apply to companies headquartered outside the EU. While MNEs based within the European Union would be fully subject to the new rules, those incorporated elsewhere would be beyond the direct force of European law except for any branches or subsidiaries within the EU. The discrepancy in the information that the two categories of multinationals could be forced to disclose publicly could create a competitive imbalance between large companies based within the EU, and those headquartered elsewhere.

4.13 As an amendment to the Accounting Directive, the Commission proposal is based on Article 50 of the Treaty on the Functioning of the EU (TFEU) on company law, rather than Article 115 TFEU, which covers corporation tax policy. This is important, because the procedures that govern the adoption of new EU legislation under these respective Articles are different. New rules under Article 115 TFEU would require unanimity in the EU's Council of Ministers—giving each Member State a veto—and limits the European Parliament to a consultative role only. By contrast, Article 50 TFEU only requires a Qualified Majority in the Council and gives the Parliament full co-legislative powers, meaning the Member States and MEPs jointly need to agree on the text of the legislation.

The European Parliament's position

4.14 The European Parliament agreed its position on the draft Directive in July 2017. MEPs supported the general objective of the Commission proposal, but put forward several amendments for discussion with the Member States.

4.15 In particular, the Parliament called for a full, global, country-by-country breakdown of tax payments by large companies within the scope of the new disclosure requirement (rather than permitting an aggregated view for non-EU countries not listed by the EU as tax havens). MEPs also voted in favour of the inclusion of other types of data in the reports, including on fixed assets, subsidies received (including preferential tax treatment), and political donations made. However, MNEs would be able to request an exemption from individual EU Member States to be allowed to omit any information otherwise due to be published, where this would be prejudicial to their commercial interests.

The Council of Ministers' position

4.16 Compared to the European Parliament, negotiations on the legal text of the Directive in the Council of Ministers have been protracted, because of opposition from a number of Member States. The choice of legal basis has been particularly controversial, with a number of countries—Ireland and Luxembourg in particular—having argued that the draft Directive in effect constitutes a tax measure, and should therefore be based on Article 115 TFEU (giving each country a veto). Germany also opposed the proposal, the sole large Member State to do so.

4.17 The question of the appropriate legal base is also likely to reflect underlying concerns about the substance of the Directive. The disclosure requirement could show that certain Member States account for a disproportional slice of the tax payments of certain multinational companies within the EU compared to the size of their economy and

domestic market.[45] Some countries have also warned that a unilateral EU approach could put European companies at a disadvantage compared to their competitors headquartered in non-EU jurisdictions. For these, the public reporting requirement would not apply to their global activities, and they may refuse to comply with any disclosure requirements other than for their operations within the EU (and not, for example, in relation to their use of non-EU tax havens). In a similar vein, EU-based companies may also be forced to publish commercially sensitive information that their non-EU competitors do not.

4.18 Even under the Qualified Majority voting rules applicable to draft EU legislation under Article 50 TFEU, a minority of Member States can still block the adoption of news laws. By late 2019, it was reported that at least 13 EU countries still opposed the proposal, sufficient to block its progress within the Council of Ministers. However, shifts in the political situation in a number of these countries have meant that this blocking minority no longer exists. At a meeting of EU Business Ministers on 25 February 2021, a number of Member States that had previously opposed the draft Directive confirmed they had changed their position. As a result, a "clear majority" of EU countries provisionally approved a revised version of the CbC Reporting Directive on 3 March 2021, allowing for negotiations with the European Parliament on the final text of the legislation to begin. Eight EU countries, including Ireland and Sweden, still publicly opposed the proposal on the grounds that it should be treated as tax legislation under the Treaties.[46]

4.19 To deal with the concerns expressed about the legal base, the revised draft Directive endorsed by a majority of EU countries emphasises that the legislation "aims to enhance corporate transparency" (rather than ultimately reducing tax avoidance) "for the protection of the interests of [shareholders] and others", where "others" is interpreted to include the company's competitors as well as the "general public". There are also substantive amendments: the Member States want to dispense with the power for the Commission to adopt a list of non-EU tax havens for which MNEs would have to publish their tax affairs. However, they have not followed the Parliament's suggestion that the CbC disclosure requirement should be broken down for each tax jurisdiction globally in which the company operates. Instead, they want to maintain public CbC reporting only for EU countries and for jurisdictions listed on the EU's existing list of non-cooperative tax jurisdictions, which is agreed twice a year by the Member States acting unanimously (giving each EU country a veto over changes to the list). For all other countries, the report would—as in the Commission's original proposal—have disclosed the company's tax payments and other information in aggregate.

45 The Council of Minister's own Legal Service (CLS), in Council document 14384/16, in November 2016 also questioned the validity of the Article 50 TFEU legal base, arguing that the Commission proposal was intended to "deter tax avoidance by exposing the companies concerned to public scrutiny of their relevant choices and policies", to be achieved by making "mandatory the disclosure of information dealing either with the payment of taxes". As such, by proposing it as a company law measure, the Commission had "mixe[d] aims and means". Instead, "since both the aim and the content of the proposal relate to [tax] and since the proposal directly affects the establishment and the functioning of the internal market, the proposal must be based on Article 115 TFEU". Member States and the legal service also questioned the empowerment for the Commission to adopt a Delegated Act listing tax havens.

46 The eight EU countries still publicly opposing the CbC Reporting Directive in its current form are Croatia, Cyprus, the Czech Republic, Hungary, Ireland, Malta and Sweden.

Further negotiations

4.20 As noted, the support given by a majority of EU countries to a revised version of the Directive in February 2021 means that negotiations with the European Parliament on the final text of the CbC legislation have now begun. Agreement between these two institutions is a prerequisite for the new country-by-country tax reporting requirement to take effect as a matter of EU law.

4.21 However, given the different positions taken by the Parliament and Council, for example in relation to the information to be included in the tax report and whether the country-by-country breakdown should be global or limited, it is unclear when they may reach agreement. The Austrian and German Governments are also still reported to be sceptical about the Directive, although they did not publicly oppose at the meeting of EU Business Ministers in February 2021. Moreover, even if the legislation is adopted on the basis of Article 50 TFEU, any Member State that feels its legal prerogatives have been infringed—because it believes the Directive should have been adopted by unanimity under Article 115 TFEU—could lodge a legal challenge before the EU Court of Justice to seek annulment of the law.

Implications of the draft EU CbC Directive for the UK

4.22 The UK of course left the European Union on 31 January 2020, and therefore any new EU legislation on country-by-country reporting of a company's tax affairs would not apply in or to the UK. However, the Government has been supportive of international efforts to introduce public country-by-country reporting for multinationals.

4.23 When the European Commission first published the draft CbC Reporting Directive in 2016, the Government told Parliament that the proposed EU approach was "appropriate and proportionate" to address aggressive tax planning by MNEs because "the nature of globally mobile firms and capital, a coordinated multilateral approach is necessary to effectively deal with the issue". It also specifically noted that an EU-wide approach would allow the UK to introduce country-by-country reporting, because "EU agreement reduces the impact on the UK's competitiveness because the requirements for public CbC reporting would be introduced across all Member States".[47] Indeed, the then-Government believed that there was a "case to go further than the current proposal and require MNEs to publish breakdowns of both their EU and non-EU operations"—as now proposed by the European Parliament—to "allow the public to see the tax paid and profits made for each country in which a MNE operates".

4.24 Now that the UK has exited the EU, the Government has maintained existing public country-by-country requirements for banks and the extractive industries that were initially introduced under EU law.[48] It has also maintained the requirement for companies to submit information to HM Revenue & Customs (HMRC) on their tax affairs in

47 The Minister told us that the Commission's proposal was "in line with the Government's objective of further enhancing tax transparency by introducing public CbC reporting on a multilateral basis. In 2016, then Chancellor (George Osborne) pressed his EU and international counterparts at the ECOFIN Council and G20 meetings to push for the details of tax paid by MNEs to be made publicly available on a CbC basis.

48 See the Capital Requirements (Country-by-Country Reporting) Regulations 2013 and the Reports on Payments to Governments Regulations 2014.

different jurisdictions on a confidential basis. The UK also continues to exchange this information with the tax authorities of certain other countries that apply OECD standards on confidentiality of taxpayers' information, including all 27 EU Member States.[49]

4.25 The Finance Act 2016[50] already allows the Treasury, by regulations, to require a company's group *public* tax strategy to include a CbC report with the information that it is already required to submit confidentially to HMRC.[51] However, the Government has to date ruled out the unilateral introduction of public country-by-country reporting by all large multinationals operating in the UK using these powers. Then-Financial Secretary Rt Hon. Mel Stride MP said in November 2017 that a move to country-by-country reporting unilaterally "would certainly make the UK less competitive than other tax jurisdictions",[52] although he added that the Government would "continue to work towards bringing in […] public country-by-country reporting".[53] More recently, in December 2020, Treasury Minister John Glen MP told the House that "only a multilateral approach would be effective in achieving transparency objectives, and avoiding disproportionate impacts on the UK's competitors or distortions regarding group structures".[54]

4.26 As noted, one of the key issues that has held up the talks in Brussels were concerns about the impact of the CbC Reporting Directive on the competitiveness of EU companies. EU law, by definition, will not have legal force in non-Member States. That means that under the proposed Directive, only EU-headquartered MNEs would be subject to the full CbC reporting obligation for all their activities worldwide. Large companies based overseas—for example in the US or the UK—could refuse to disclose the information except in relation to their specific activities within the EU. Fears about the impact that might have on competitiveness is also why the UK Government has to date ruled out introducing public CbC disclosures unilaterally. Therefore, if the UK were to introduce country-by-country reporting as well, this would be beneficial from the EU's perspective because it would extend the full CbC disclosure requirement to UK-headquartered multinationals and to the UK activities of non-EU, non-UK MNEs, which the EU Directive could not fully capture. The same would of course also apply vice versa for the UK.

49 The UK CbC regime is set out in s122 of the Finance Act 2015 and SI 2016/237, based on model legislation published by the OECD, as part of the BEPS project in Transfer Pricing Documentation and Country-by-Country Reporting, Action 13 (5 October 2015). HMRC reviewed the financial implications of implementing the OECD CbC reporting model in the UK for the Autumn Statement 2014—the measure was estimated to yield £45 million over the five-year period, 2015–16 to 2019–20.

50 Paragraph 17(6) of schedule 19 to the Finance Act 2016.

51 During the report stage of the Finance Bill in September 2016, the Government accepted a proposed amendment from Caroline Flint to, in her words, "enshrine in law support for the principle of public country-by-country reporting with the power for the Government to introduce when the time is most appropriate." (HC Deb 5 September 2016 c136).

52 In particular, the Minister argued the UK would not be able to "get public disclosure if a UK company had associated non-UK companies in other jurisdictions and not under that company's control" and "the big advantage of going multilaterally is the standardisation of the standards that we set and the rules and regulations around each particular step".

53 The Minister made the comments in a Westminster Hall debate in November 2017 on country by country reporting: HC Deb 22/11/2017 c462WH.

54 The Minister made his remarks in a debate on the Financial Services Bill, in relation to a clause proposed by the Opposition which would have required the Treasury to produce an annual report on "its progress in pursuit of international action on public country-by-country reporting". He argued that "it would not be appropriate for the Treasury to provide a detailed report each year assessing the status and evaluating the progress of fast-moving, complex discussions that typically take place between countries on a confidential basis".

4.27 The new UK/EU Trade & Cooperation Agreement (TCA) reiterates both sides' support the OECD's 2015 BEPS Action Plan, on which the draft EU CbC Reporting Directive builds, but does not specify any particular legal commitments or actions to be undertaken by the UK and EU jointly in this area.[55] The Government does not appear to have commented publicly on the decision by the EU Member States in February 2021 to proceed with the introduction of general public CbC reporting for multinational enterprises under EU law, although negotiations on the substance of the Directive are of course on-going. Consequently, it is unclear if the UK would be willing to discuss cooperating with the European Union in this area if new rules are agreed at EU-level, with a view to also introducing new tax disclosure rules for multinationals in the UK under the Finance Act 2016 as part of a wider international effort. Any prospect of UK-EU cooperation in this area will of course also be influenced by the wider state of the bilateral relationship, which is currently characterised by tensions and disputes (not least over the Northern Ireland Protocol).

Conclusions and action

4.28 After nearly five years of negotiations, a majority of the remaining 27 Member States of the EU now support the introduction of public country-by-country reporting of the tax affairs of large multinationals with operations within the European Union. However, potentially difficult negotiations still lie ahead before the new CbC Reporting Directive can take effect, as the positions of the European Parliament and the Member States need to be reconciled, in particular on the granularity of the country-by-country reports. It is therefore unclear when any new tax disclosure requirements for multinationals may become law within the EU.

4.29 The Government was broadly supportive of the draft Directive when the UK was still a Member State and indeed had taken the position that the legislation should go further, mandating a full, global, country-by-country breakdown of the tax paid by multinationals active in the EU (rather than only for individual EU countries and 'blacklisted' tax jurisdictions). Ministers have repeatedly confirmed their commitment to public CbC reporting as part of a multilateral approach, to avoid any disproportionate effect on the competitiveness of UK companies and to increase the effectiveness of such disclosures.

4.30 To our knowledge however, the Government has not publicly commented on the latest developments in the EU's Council of Ministers that may, in the medium term, result in the first multilateral commitment to public country-by-country reporting for MNEs. We have therefore written to the Financial Secretary to the Treasury to clarify the Government's current views on the merits of the draft EU Directive on public country-by-country reporting, and whether it is considering possible cooperation with the EU if the latter adopts legislation to that effect to enable CbC reporting to be introduced in the UK as part of a multilateral effort.

4.31 The proposed introduction of public CbC reporting requirements for multinationals is only one of various measures being pursued at EU-level (and internationally) to address tax avoidance and evasion. For example, separate discussions are on-going about the taxation of the digital economy, where base erosion and profit shifting is especially pronounced, and the EU recently announced that it would try to establish a joint approach

55 Article LPFS.5.2 TCA on taxation standards.

with the United States on this issue. The European Commission is also due to publish an "Action Plan" on EU corporate taxation policy later in 2021. Given its economic proximity to the Single Market, the UK could still be affected by changes in the EU's approach to international tax issues. We will continue to consider the implications of other EU policy measures in this field for the UK separately, where appropriate.

4.32 In the interim, in anticipation of the Minister's reply to our questions about public CbC reporting, we draw these developments to the attention of the Business, Energy and Industrial Strategy Committee, the Public Accounts Committee and the Treasury Committee.

Letter from the Chair to the Financial Secretary to the Treasury (Rt Hon. Jesse Norman MP)

You will be aware that the EU's Council of Ministers on 25 February gave its political endorsement to a draft Directive to introduce public country-by-country (CbC) reporting of the tax affairs of the largest multinationals with operations within the European Union.[56] We understand talks are now underway with the European Parliament on the final text of the legislation.

The UK has consistently underlined the merits of public CbC reporting as part of a toolbox against aggressive tax avoidance by large companies. While the Treasury already has the power to introduce such disclosure requirements under the Finance Act 2016, the Government has been clear that it is not persuaded of the merit of the UK doing so unilaterally, not least because of the impact on the UK's international competitiveness. Your predecessor told us in 2016—obviously in a very different political and legal context –that an agreement at EU-level would reduce "the impact on the UK's competitiveness" of new requirements for public CbC reporting, because they would be introduced by a large group of countries simultaneously. Your colleague, the Economic Secretary, also reiterated as recently as December 2020 that the Government was still pursuing a "multilateral approach" in this area.

While there is of course no suggestion that the UK would be required to implement any new EU Directive on public CbC reporting, it is still open to the Government to engage with the EU to seek to influence the substance of the envisaged CbC reporting disclosures with a view to a joint approach, or indeed to introduce such an obligation unilaterally once the EU adopted its own legislation to that effect. We recognise that the scope for any such cooperation will also be influenced by the state of the wider UK/EU relationship, but focus here on the substantive merits of the policy the EU is pursuing in this area.

In light of this, we would ask you to clarify the Government's current view on the EU's efforts to introduce public CbC reporting for multinationals and the recent developments in the Council of Ministers. In particular, we would welcome information on:

- whether or not the future introduction of mandatory CbC reporting throughout the EU could allow for the UK to also introduce such a requirement (since it would take effect in a significant number of jurisdictions at the same time and therefore have less of an impact on the UK's competitiveness), and the Government's basis for that assessment;

56 EU Document COM(2016), 7949/16 (37663).

- whether the Government has recently engaged, or is planning to engage, with the EU on the substance of its Directive, as a key international initiative on public CbC reporting; and
- if there are other international initiatives on public CbC reporting on-going which the Government believes would be preferable as the basis for the introduction of such disclosures under UK law, and if so, which.

We look forward to your response by 9 April 2021.

5 Documents not considered to be legally and/or politically important

Department for Digital, Culture, Media and Sport

(41701) — COM(20) 784	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Europe's Media in the Digital Decade: An Action Plan to Support Recovery and Transformation.

HM Treasury

(41793) 6145/21 COM(2021) 53	Proposal for a Council Implementing Decision authorising the United Kingdom in respect of Northern Ireland to apply a special measure derogating from Articles 16 and 168 of Directive 2006/112/EC on the common system of value added tax.

Annex

Documents drawn to the attention of select committees:

('SNC' indicates that scrutiny (of the document) is not completed'; 'SC' indicates that scrutiny of the document is completed)

Business, Energy and Industrial Strategy Committee: Public country-by-country tax reporting of multinationals in the EU [Proposed Directive (SNC)]; Data adequacy [Proposed Implementing Decisions (SNC)]

Defence Committee: Cybersecurity: EU Strategy and revised Network and Information Systems Directive [(a) Joint Communication, (b) Proposed Directive (SNC)]

Digital, Culture, Media and Sport Committee: Cybersecurity: EU Strategy and revised Network and Information Systems Directive [(a) Joint Communication, (b) Proposed Directive (SNC)]; Data adequacy [Proposed Implementing Decisions (SNC)]

Foreign Affairs Committee: Cybersecurity: EU Strategy and revised Network and Information Systems Directive [(a) Joint Communication, (b) Proposed Directive (SNC)]

Home Affairs Committee: Cybersecurity: EU Strategy and revised Network and Information Systems Directive [(a) Joint Communication, (b) Proposed Directive (SNC)]; Data adequacy [Proposed Implementing Decisions (SNC)]

Joint Committee on Human Rights: Data adequacy [Proposed Implementing Decisions (SNC)]

International Development Committee: Northern Ireland Protocol: Market access for goods from African, Caribbean and Pacific (ACP) countries [Commission Report (SC)]

International Trade Committee: Northern Ireland Protocol: Market access for goods from African, Caribbean and Pacific (ACP) countries [Commission Report (SC)]; Data adequacy [Proposed Implementing Decisions (SNC)]

Northern Ireland Affairs Committee: Northern Ireland Protocol: Market access for goods from African, Caribbean and Pacific (ACP) countries [Commission Report (SC)]; Data adequacy [Proposed Implementing Decisions (SNC)]

Public Accounts Committee: Public country-by-country tax reporting of multinationals in the EU [Proposed Directive (SNC)]

Science and Technology Committee: Data adequacy [Proposed Implementing Decisions (SNC)]

Treasury Committee: Public country-by-country tax reporting of multinationals in the EU [Proposed Directive (SNC)]

Formal Minutes

Wednesday 17 March 2021

Members present:

Sir William Cash, in the Chair

Jon Cruddas	Mr David Jones
Richard Drax	Craig Mackinlay
Margaret Ferrier	Anne Marie Morris
Mrs Andrea Jenkyns	Greg Smith

Scrutiny Report

Draft Report, proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1.1 to 5 read and agreed to.

Resolved, That the Report be the Fortieth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

[Adjourned till Wednesday 24 March at 1.45 p.m.

Standing Order and membership

The European Scrutiny Committee is appointed under Standing Order No.143 to examine European Union documents and—

a) to report its opinion on the legal and political importance of each such document and, where it considers appropriate, to report also on the reasons for its opinion and on any matters of principle, policy or law which may be affected;

b) to make recommendations for the further consideration of any such document pursuant to Standing Order No. 119 (European Committees); and

c) to consider any issue arising upon any such document or group of documents, or related matters.

The expression "European Union document" covers—

i) any proposal under the Community Treaties for legislation by the Council or the Council acting jointly with the European Parliament;

ii) any document which is published for submission to the European Council, the Council or the European Central Bank;

iii) any proposal for a common strategy, a joint action or a common position under Title V of the Treaty on European Union which is prepared for submission to the Council or to the European Council;

iv) any proposal for a common position, framework decision, decision or a convention under Title VI of the Treaty on European Union which is prepared for submission to the Council;

v) any document (not falling within (ii), (iii) or (iv) above) which is published by one Union institution for or with a view to submission to another Union institution and which does not relate exclusively to consideration of any proposal for legislation;

vi) any other document relating to European Union matters deposited in the House by a Minister of the Crown.

The Committee's powers are set out in Standing Order No. 143.

The scrutiny reserve resolution, passed by the House, provides that Ministers should not give agreement to EU proposals which have not been cleared by the European Scrutiny Committee, or on which, when they have been recommended by the Committee for debate, the House has not yet agreed a resolution. The scrutiny reserve resolution is printed with the House's Standing Orders, which are available at www.parliament.uk.

Current membership

Sir William Cash MP (*Conservative, Stone*) (Chair)

Tahir Ali MP (*Labour, Birmingham, Hall Green*)

Jon Cruddas MP (*Labour, Dagenham and Rainham*)

Allan Dorans MP (*Scottish National Party, Ayr Carrick and Cumnock*)

Richard Drax MP (*Conservative, South Dorset*)

Margaret Ferrier MP (*Scottish National Party, Rutherglen and Hamilton West*)

Mr Marcus Fysh MP (*Conservative, Yeovil*)

Mrs Andrea Jenkyns MP (*Conservative, Morley and Outwood*)

Mr David Jones MP (*Conservative, Clwyd West*)

Stephen Kinnock MP (*Labour, Aberavon*)

Mr David Lammy MP (*Labour, Tottenham*)

Marco Longhi MP (*Conservative, Dudley North*)

Craig Mackinley MP (*Conservative, South Thanet*)

Ann Marie Morris MP (*Conservative, Newton Abbot*)

Charlotte Nichols MP (*Labour, Warrington North*)

Greg Smith MP (*Conservative, Buckingham*)